

PCT

REC'D 26 MAY 2004

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

PCT



(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PWO-0850	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/CA 02/01947	International filing date (day/month/year) 13.12.2002	Priority date (day/month/year) 26.12.2001
International Patent Classification (IPC) or both national classification and IPC G06F1/00		
Applicant RESEARCH IN MOTION LIMITED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.
- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:
- I ☒ Basis of the opinion
 - II ☐ Priority
 - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain documents cited
 - VII ☐ Certain defects in the international application
 - VIII ☐ Certain observations on the international application

Date of submission of the demand 13.06.2003	Date of completion of this report 25.05.2004
Name and mailing address of the International preliminary examining authority:  European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax +31 70 340 - 3016	Authorized Officer Fleckinger, C Telephone No. +31 70 340-3416 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/CA 02/01947**

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-9 as originally filed

Claims, Numbers

1-17 filed with telefax on 28.04.2004

Drawings, Figures

1/4-4/4 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:
- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
4. The amendments have resulted in the cancellation of:
- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/CA 02/01947

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

see separate sheet

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-17
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	1-17
Industrial applicability (IA)	Yes: Claims	1-17
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item I

Basis of the report

The amendments filed by fax the 28th of April 2004 are not allowable under Article 34(2)(b) PCT since the added feature "tamper-resistant internal memory" is not directly and unambiguously disclosed in the original description. Furthermore, the applicant has not provided any basis in the application document as filed for the amendments.

This report is therefore based on the originally filed set of claims.

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: EP-A-0 816 970 (SUN MICROSYSTEMS INC) 7 January 1998 (1998-01-07)

D2: US-A-5 805 882 (LE HUNG Q ET AL) 8 September 1998 (1998-09-08)

1 The document D1 discloses (the references in parentheses applying to this document):

A boot method suitable for use in a mobile device having FLASH memory ("flash PROM", col.4 l.21) storing boot instructions ("micro-code instruction", col.4 l.26-27 and l.31-32) comprising the step of:

reading (implicit when the decryptor applies the digital signature, col.4 l.45-48) contents of a security location ("signature", col.4 l.51-55) in the FLASH memory (fig.2, item 57);

comparing security values (col.5 l.49-50).

Claim 1 differs principally from D1 in that the serial port is selectively polled based on the result of a comparison of security values.

In D1, when the security values are not equal, this means that the boot instructions are not valid.

Starting from D1, the problem to be solved by the present invention may therefore be regarded as how to obtain valid boot instructions.

In seeking to solve the problem of obtaining valid boot instruction, the skilled person would consult D2 because it addresses exactly this problem and comes from the same

technical field (D2: col.2 l.67-col.3 l.4; col.3 l.19-26).

The skilled person would then implement the recovery solution of D1 (col.5 l.54-58) using the features of D2 of checking if a flash ROM programming sequence is present at the data port and updating the flash ROM (D2: col. 3 l.18-25). The skilled person would thereby selectively poll a data port for activity based on the result of the comparison and arrive at a method differing only in obvious choices from claim 1. More specifically, the choice of using a serial port as data port instead of the parallel port used in D2 is a matter of normal design procedure.

The remaining difference with the method of claim 1 is that the cryptographic feature (computing hash codes) has been omitted in claim 1. Apart from the obviously and consequently simpler design of the method of claim 1, the only result of the omission of the cryptographic feature is that the effects related to cryptography are no longer present in the method according to claim 1. The skilled person would therefore whenever necessary or more appropriate use the well-known basic check of comparing contents of security location with a predetermined security value (which could be the "public key") instead of using the comparison and authentication methods of D1. Such a simplification does not involve an inventive step (Articles 52(1) and 56 EPC).

Applying a similar reasoning for the corresponding apparatus, the skilled person would arrive at an apparatus falling within claim 9.

The subject-matter of **independent claims 1 and 9** can therefore not be considered as involving an inventive step (Article 33(3) PCT).

2 Dependent claims 2-8 and 10-17 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty or inventive step (Article 33(3) PCT).

Features of dependent claims 2-8 and 10-17 are several straightforward possibilities which comes within the scope of the customary practice followed by the skilled person.

PCT/CA02/01947

What is claimed is:

1. A boot method for use in a mobile device having FLASH memory storing boot instructions, having tamper-resistant internal memory, and having a serial port,
5 comprising the steps of:
 reading a key value from a security location in the FLASH memory;
 comparing the key value to a predetermined security value stored in the tamper-resistant internal memory; and
 selectively polling the serial port for activity based on the result of the
10 comparison.
2. A boot method according to claim 1 wherein the polling is performed if the key value does not match the predetermined security value.
- 15 3. A boot method according to claim 1 further comprising the step of jumping to a boot location in FLASH memory to execute instructions stored therein.
4. A boot method according to claim 2 further comprising the step of downloading code into internal SRAM located in the mobile device in response to a
20 detection of serial port activity.
5. A boot method according to claim 4 further comprising the step of executing an instruction in the downloaded code.
- 25 6. A boot method according to claim 5 further comprising the step of jumping to a boot location in FLASH memory to execute boot instructions stored therein.
7. A boot method according to claim 1 wherein the predetermined security value is stored in a BootROM located in the mobile device.

30

- 10 -

BEST AVAILABLE COPY

Empf.zeit:28/04/2004 17:57

Empf.nr.:216 P.008

AMENDED SHEET

PCT/CA02/01947

8. A boot method according to claim 1 wherein the step of reading is performed in response to a reset command.
9. An apparatus for use in a mobile device having a serial port, comprising:
- 5 a first, tamper-resistant, memory means having a predetermined security value stored therein;
- a second memory means having a security location for storing a key value;
- and
- a processor in communication with the first and second memory means for
- 10 comparing a key value stored in the security location to the predetermined security value, and for selectively polling the serial port for activity based on the result of the comparison.
10. An apparatus according to claim 9 wherein the first, tamper-resistant, memory
- 15 means comprises a Boot Read Only Memory (BootROM).
11. An apparatus according to claim 9 wherein the second memory means comprises a FLASH memory.
12. An apparatus according to claim 9 further comprising a reset means in
- 20 communication with the processor for initiating a reset process.
13. An apparatus according to claim 9 wherein the processor compares the key value and said predetermined security value in response to initiation of a reset
- 25 process.
14. An apparatus according to claim 9 wherein the first, tamper-resistant, memory means is located on an ASIC.
15. An apparatus according to claim 9 wherein the processor is located on an
- 30 ASIC.

- 11 -

BEST AVAILABLE COPY

Empf.zeit:28/04/2004 17:57

Empf.nr.:216 P.009

AMENDED SHEET

PCT/CA02/01947

16. An apparatus according to claim 9 wherein the processor comprises a microcontrol unit connected to the serial port.
- 5 17. An apparatus according to claim 9 wherein the processor comprises a digital signal processor connected to the second memory means.

- 12 -

BEST AVAILABLE COPY

Empf.zeit:28/04/2004 17:57

Empf.nr.:216 P.010

AMENDED SHEET



Saioudi

Name: **Nabila Saioudi**

Address: **The Hague Shell, Room S08A15, Tel: 2448**

Userid: NS03411

Printer or e-mail address: P0116

Format: PS

Requested: 19/05/04 14:37:22

JobNo: job

Batch: 1 of 1

CA0201947

Epoline Phoenix printout 27913588

BEST AVAILABLE COPY